

REMARKS

Claims 1-41 are pending in this application. By this amendment, Applicants have amended claims 1, 21, 25, 33, 34, 39 and 40.

Reconsideration of the above-identified application in view of the foregoing amendments and the following remarks is respectfully requested.

Rejections Under 35 U.S.C. § 112, ¶1:

In the Office Action, claims 2 and 3 were rejected under 35 U.S.C. § 112, ¶1 as allegedly failing to comply with the written description requirement. In particular, the Office Action asserts that:

“Claim 2 recites the limitation ‘wherein the first decryption information corresponds to a seed of a macro period’. Claim 2 is dependent upon claim 1, which recites the amended feature ‘wherein the first decryption information decrypts the service’. The originally filed specification does not disclose that the seed of a macro period decrypts the service. The specification only discloses that the seed of a macro period decrypts the key of the first micro period of the macro period (page 6, last paragraph; figure 2).”

Applicants respectfully submit that the specification adequately supports the subject matter of claim 2 and, in particular, discloses the claimed feature of the seed of a macro period decrypting the service. That feature is illustrated in the instant application, e.g., on p. 8, 1st full paragraph & Figure 5, wherein it is provided:

“As shown in FIG. 5, at some point in advance of the service transmission start time “t0”, user A connects to service provider 10 via the bi-directional channel and receives *a seed 20a for decrypting a service*. At the service transmission start time “t0”, user A begins *using the seed 20a to decrypt the service*. At some point in advance of the first micro period 24a start time “t1”, user A will receive updated decryption information over the uni-directional channel for use in decrypting the service during the first micro period 24a. The updated decryption information will be encrypted using the seed 20a.” (emphasis added)

Accordingly, Applicants respectfully submit that the subject matter of claim 2 is clearly supported by the specification of the instant application, and thus, respectfully request that the rejections of claims 2 and 3 be withdrawn.

Also in the Office Action, claims 33 and 34 were rejected under 35 U.S.C. § 112, ¶1 as allegedly failing to comply with the enablement requirement. Applicants have amended claims 33 and 34 in that regard to include the features of “attempting to re-receive the service” and “upon re-receiving the service, determining whether either the first decryption information or the second decryption information is valid decryption information.” Applicants respectfully submit that these features are supported by the disclosure at, e.g., p. 14, last paragraph and p. 15 first full paragraph of the instant application wherein after the service has been dropped, the client 12 determines whether the current decryption information is still valid through, e.g., “trial and error” and, if still valid, continues to decrypt the service using the valid decryption information. One of ordinary skill in the art would have understood that in order to be able to determine the validity of the of the current decryption information through trial and error, the client would have to attempt to re-receive the service.

Accordingly, Applicants respectfully submit that claims 33 and 34 comply with the enablement requirement of 35 U.S.C. § 112, ¶1 and thus request that the foregoing rejections be withdrawn.

Rejections Under 35 U.S.C. §102:

In the Office Action, claims 1-3, 6-9, 12, 13, 16-19, 21, 25, 26, 28, 29, 35-36 and 39-41 were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,510,515 to Raith (“Raith”). Claims 1, 21, 25, 39 and 40 are independent.

Applicants' invention, as defined by amended claim 1, is directed to a method for a service provider to transmit decryption information in a secure manner. Claim 1, as amended, calls for "transmitting the second decryption information over the unidirectional channel, wherein the second decryption information decrypts the service; and transmitting the service, encrypted with encryption information corresponding to the second decryption information rather than with encryption information corresponding to the first decryption information, over the unidirectional channel." The Office Action appears to equate the "service key" and the "secret variable" of Raith with "the first decryption information" and "the second decryption information", respectively, of claim 1.

In contrast with Applicant's invention as defined by amended claim 1, however, the service in Raith appears to always be encrypted in accordance with the service key. The secret variable simply provides an additional layer of encryption. As such, Raith does not teach or suggest "transmitting the service, encrypted with encryption information corresponding to the second decryption information rather than encryption information corresponding to the first decryption information, over the unidirectional channel."

Accordingly, claim 1 is not anticipated by Raith for this reason alone.

In addition, however, the secret variable in Raith does not decrypt the service, and thus, is not "second decryption information [that] decrypts the service", as further required by claim 1. Instead, the use of the secret variable in Raith merely results in an encrypted version of the service.

Accordingly, claim 1 is not anticipated by Raith for this additional reason.

Claims 21, 25, 39 and 40 contain features similar to those found in amended claim 1, and thus, are allowable for similar reasons.

Rejections Under 35 U.S.C. §103:

In the Office Action, claims 1, 4-8, 11, 13-27, 29-36 and 39-41 were rejected under 35 U.S.C. §103 as being unpatentable over U.S. Patent No. 6,516,412 to Wasilewski et al. in view of U.S. Patent No. 5,619,274 to Roop et al. Claim 9 was rejected under §103 as being unpatentable over Wasilewski and Roop in view of U.S. Patent No. 6,748,082 to Vieweg. Claim 10 was rejected under §103 as being unpatentable over Wasilewski and Roop in view of U.S. Patent No. 6,925,562 to Gulcu et al. Lastly, claim 12 and 28 were rejected under §103 as being unpatentable over Wasilewski and Roop in view of Raith. Claims 1, 21, 25, 39 and 40 are independent.

The Office Action asserts that Wasilewski discloses all of the subject matter of claim 1, except “an initial control word [that] is included in the authorization message”. In that regard, the Office Action appears to allege that an Entitlement Control Message (ECM) of Wasilewski, which contains a code word encrypted using the multi session key (MSK), corresponds to the second decryption information of claim 1. The Office Action then alleges that it would have been obvious in view of Roop to modify Wasilewski to include an “initial” control word in the authorization message (i.e., in the Entitlement Management Message (EMM)), which contains an encrypted version of the MSK) because “[w]ith the initial control word in hand, the requestor’s device would be ready to decrypt the service when it was first received”. It appears that the Office Action’s position is that the initial control word would then correspond to the first decryption information of claim 1.

Applicants respectfully disagree and assert that there is no motivation in the cited references to modify Wasilewski in the manner suggested in the Office Action. The alleged motivation is that “[w]ith the initial control word in hand, the requestor’s device would be ready

to decrypt the service when it was first received.” However, in Wasilewski, the set-top box is always “ready” to decrypt the service upon receipt since there is no unacceptable, or even perceptible, delay disclosed in Wasilewski in generating the codeword used to decrypt the service from the ECM that would warrant modifying the EMM to include an “initial” codeword.. Indeed, one method used in Wasilewski for transmitting the encrypted code word to the set-top box is in a multiplexed transmission containing the program encrypted with the codeword, the ECM including the code word encrypted with the MSK and the EMM including the encrypted MSK, all without any hint of processing delay associated with generating the codeword at the set top box. The alternative disclosed in Wasilewski is to send the MSK to the set-top box in the EMM via a separate channel, but this too is not disclosed as presenting any delay in generating the codeword from the ECM. Nor do the cited passages of Roop teach or suggest that sending a decryption key in an authorization message makes the requestor’s device any meaningfully more “ready” to decrypt the service when it is first received such that one would have been motivated to modify the method of Wasilewski in that regard.

Accordingly, for at least the foregoing reasons, Applicants respectfully submit that claim 1 is patentable over the combination of Wasilewski and Roop.

Claims 21, 25, 39 and 40, contain features similar to those found in amended claim 1, and thus, are allowable for at least the same reasons as set forth above in urging the allowance of amended claim 1. In addition, with respect to claim 39, the code word of Wasilewski is not “installed ... on a device of the requestor”, as required by claim 39, but instead is generated by the set-top box (see, e.g., Fig. 1, reference numeral 119), and thus, claim 39 is not anticipated by Wasilewski for this additional reason.

Dependent Claims:

Applicants do not believe it necessary at this time to address the rejections of the dependent claims as Applicants believe that the foregoing places the independent claims in condition for allowance. Applicants, however, reserve the right to address those rejections in the future should such a response be deemed necessary and appropriate.

CONCLUSION

Applicants respectfully submit that this Application is in condition for allowance for which action is earnestly solicited.

If a telephone conference would facilitate prosecution of this Application in any way, the Examiner is invited to contact the undersigned at the number provided.

AUTHORIZATION

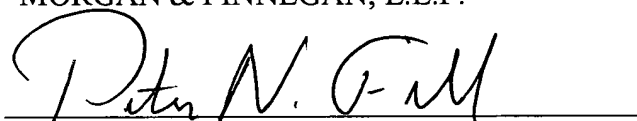
The Commissioner is hereby authorized to charge any additional fees which may be required by this response, or credit any overpayment to Deposit Account No. 13-4500, Order No. 4208-4027.

In the event that an extension of time is required, or which may be required in addition to that requested in a petition for an extension of time, the Commissioner is requested to grant a petition for that extension of time which is required to make this response timely and is hereby authorized to charge any fee for such an extension of time or credit any overpayment for an extension of time to Deposit Account No. 13-4500, Order No. 4208-4027.

Respectfully submitted,
MORGAN & FINNEGAN, L.L.P.

Dated: December 20, 2006

By:


Peter N. Fill
Registration No. 38,876

Correspondence Address:

MORGAN & FINNEGAN, L.L.P.
3 World Financial Center
New York, NY 10281-2101
(212) 415-8700 Telephone
(212) 415-8701 Facsimile